CLAIMS

1-16. (Cancelled).

17. (Previously Presented) An apparatus for determining computer security threats at least coupled to an Information Technology (IT) infrastructure, comprising:

a network scanner, wherein the network scanner at least utilizes at least one taxonomy to determine at least one possible intrusion;

an intrusion detector, wherein the intrusion detector at least detects at least one actual intrusion; and

false-positive/true-positive (FPTP) detector, wherein the FPTP detector at least compares the at least one possible intrusion with the at least one actual intrusion in order to update the at least one taxonomy.

18. (Previously Presented) The apparatus of Claim 17, wherein the FPTP detector further is at least configured to label the at least one possible intrusion as false-positive or true positive.

19. (Previously Presented) The apparatus of Claim 18, wherein the FPTP detector is at least configured to sort possible intrusions labeled as true positive.

20. (Previously Presented) The apparatus of Claim 18, wherein the FPTP detector is at least configured to prioritize possible intrusions labeled as true positive.